

IIMT
UNIVERSITY
MEERUT

Transforming Education System, Transforming Lives



IT POLICY

Policy No.:- IIMTU/RO/IQAC/2022/27

IIMT
UNIVERSITY

Transforming Education System, Transforming Lives



UGC Approved

Section 2(f) & 12B

IT POLICY
&
GUIDELINES
IIMT UNIVERSITY, MEERUT



'O' Pocket, Ganga Nagar, Mawana Road, Meerut. (U.P.) - 250001
Ph. No. 0121-2793500-506, Fax. 0121-2793600
Website : www.iimtu.com; E-mail : mail@iimtu.com

Table of Contents

S.No.	Page Np.
1. Abbreviation	3
2. Introduction	4
3. Scope	4
4. Objective	4
5. Roles and Responsibilities	5
6. Acceptable Use	6
7. Privacy and Personal Rights	7
8. Privacy in Electronic mail	7
9. User Compliance	7
10. Access to the IIMT University Network	8
11. Monitoring and Privacy	9
12. Electronic mail Access from the IIMT University Network	9
13. Access to Social Media Sites from IIMT University, Meerut Network.	9
14. Use of Information Technology Devices Issued by IIMT University, Meerut	10
15. Security Incident Management Process	10
16. Intellectual Property of IIMT University, Meerut	11
17. Enforcement	11
18. Deactivation	11
19. Audit of IIMT University, Meerut Network Infrastructure	12
20. Review	12
21. Information technology Hardware Installation Policy	12
22. Software Installation and Licensing Policy of IIMT University, Meerut	14
23. Use of Information technology devices on IIMT University, Meerut network	15
24. Network (Intranet & Internet) Use Policy	17
25. Email Account Usage Policy	20
26. Institutional Repository (IR)	21
27. Disposal of ICT equipment	23
28. Breach of this Policy	23
29. Revisions to Policy	23
30. Appendix – I: Email Requisition Form	24
31. Appendix – II: Email Requisition Form	25
32. Appendix – III: Wi-Fi Access Requisition Form	26
33. Appendix – IV: Wi-Fi Access Requisition Form	27



1. Abbreviation

Sl. No. Abbreviation Description

1.	IIMTU	IIMT University, Meerut
2.	CA	Competent Authority
3.	IA	Implementing Agency
4.	LAN	Local Area Network
5.	GoI	Government of India
6.	IT	Information Technology
7.	ICT	Information and Communication Technology
8.	IP	Internet Protocol
9.	DHCP	Dynamic Host Configuration Protocol
10.	IR	Institutional Repository
11.	EULA	End User License Agreement
12.	CAPEX	Capital Expenditure
13.	OPEX	Operational Expenditure



2. Introduction

IIMT University, Meerut provides IT resources to sustain the educational, instructional, research, and administrative activities of the University and to increase the efficiency and productivity of the employees. These resources are meant as tools to access and process information related to their areas of work.

This policy document establishes the specific requirements for the use of all Information Technology resources at IIMT University. This policy is applicable to all users of computing resources owned or managed by IIMT University, Meerut. Individuals covered by the policy include (but are not limited to) IIMT University, Meerut faculty and visiting faculty, staff, students, alumni, guests, external individuals, organizations, departments, offices, constituent Schools and Colleges and any other entity which fall under the management of IIMT University, Meerut accessing network services via IIMT University, Meerut's computing facilities.

For the purpose of this policy, the term 'Information Technology Resources' includes all University owned, licensed, or managed hardware and software, and use of the University network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Misuse of these resources can result in unwanted risk and liabilities for the University. It is, therefore, expected that these resources are used primarily for University related purposes and in a lawful and ethical way.

3. Scope

This policy governs the usage of IT Resources from an end user's perspective. This policy is applicable to all individuals/ users/ entities, which uses the Information Technology resources of IIMT University, Meerut.

4. Objective

The objective of this policy is to ensure proper access to and usage of IIMT University, Meerut's Information Technology resources. Usage of resources requires user's agreement



to be governed by this policy.

- a. This policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established.
- b. This policy establishes University-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the IIMT University, Meerut.
- c. Information assets addressed by the policy include computers, data, information systems, networking devices, intellectual property and documents.

5. Roles and Responsibilities

The following roles and responsibilities are expected from each entity:

- 1) IIMT University, Meerut shall implement appropriate process to ensure compliance of this policy by their users. IIMT University Computer Centre shall be the implementing agency.
- 2) Computer Centre shall ensure resolution of all incidents related to the security aspects of this policy by their users. Implementing Agency shall provide the requisite support in this regard.
- 3) Use of IIMT University, Meerut information technology resources for those activities that are dependable with the academic, research and public service mission of the University and are not "Prohibited Activities".
- 4) All users shall obey the existing national, state and other applicable laws.
- 5) Abide by existing telecommunications and networking laws and regulations.
- 6) Follow copyright laws regarding protected commercial software or intellectual property. IIMT University, Meerut provides use of intellectual and/or work-related tools, including access to the Library, certain computer systems, and servers, software and databases and the World Wide Web. It is expected from University group of people to have a reasonable belief of unhindered use of these tools, of certain degrees of privacy and of protection from abuse and intrusion by others sharing these resources. Authorized users can suppose their right to access information and to say their opinion to be protected as it is for document and other



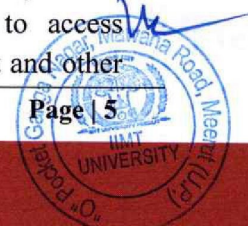
IT POLICY (Policy No. IIMTU/RO/IQAC/2022/27)

'O' Pocket, Ganga Nagar, Mawana Road, Meerut. (U.P.) - 250001

Ph. No. 0121-2793500-506, Fax. 0121-2793600

Website : www.iimtu.com; E-mail : mail@iimtu.com

Page | 5



- forms of non- electronic communication.
- 7) Users of IIMT University, Meerut shall not install any network/security device on the network without discussion with the implementing agency.
 - 8) It is responsibility of the University society to know the regulations and policies of the University that apply to appropriate use of the IIMT University's technologies and resources. IIMT University group of people is responsible for exercising good judgment in the use of the IIMT University's technological and information resources. Just because an act is technically possible does not mean that it is right to perform that action.
 - 9) As a representative of the IIMT University, Meerut society, each individual is expected to respect and uphold the IIMT University's good name and reputation in any activities related to use of ICT communications within and outside the IIMT University.
 - 10) Competent Authority of IIMT University, Meerut should ensure proper distribution and effective implantation of this policy.

6. Acceptable Use

- a. An allowed user may use only the information technology resources he/she has approval. No user should use another one's individual's account, or attempt to capture or speculate the other users' passwords.
- b. A user is individually accountable for appropriate use of all resources assigned to him/her, including the computer, the network address or port, software and hardware. Therefore, he/she is responsible to the University for all use of all such resources. As an authorized IIMT University, Meerut user, he/she should not connect in or enable not permitted users to access the network by using information technology resources of IIMT University, Meerut or a personal computer that is connected to the IIMT University, Meerut campus wide Local Area Network.
- c. The IIMT University is bound by its End User License Agreement (EULA), respecting certain third party resources.
- d. Users should make a realistic effort to protect his/her passwords and to secure resources against not permitted use or access.



(Policy No. IIMTU/RO/IQAC/2022/27)

O' Pocket, Ganga Nagar, Mawana Road, Meerut. (U.P.) - 250001

Ph. No. 0121-2793500-506, Fax. 0121-2793600

Website : www.iimtu.com; E-mail : mail@iimtu.com



- e. No user must endeavor to access limited portions of the network, an operating system, security software or other administrative applications without suitable authorization by the computer center.
- f. Users must obey the policies and guidelines for any specific set of resources to which he/she have been granted access.
- g. When other policies are more restraining than this policy, the more restraining policy takes precedence.

7. Privacy and Personal Rights

- 1) All users of the IIMT University's information technology resources are expected to respect the privacy and personal rights of others.
- 2) Do not access or copy another user's email, data, programs, or other files without permission and consent of the Competent Authority (CA).
- 3) While the IIMT University does not generally monitor or limit content of information transmitted on the campus wide local area network, it reserves the right to access and analysis of such information under certain conditions and after due approval of the competent authority.

8. Privacy in Electronic mail

While every effort is made to ensure the privacy of IIMT University email users, this may not all the time be possible. Since employees are granted use of electronic information systems and network services to conduct IIMT University business, there may be instances when the I I M T University, based on approval from competent authority, reserves and retains the right to access and inspect stored information with the permission of the user.

9. User Compliance

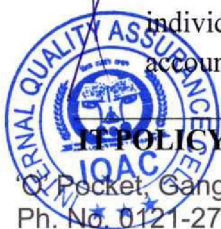
When an individual uses IIMT University, Meerut's information technology resources, and accepts any IIMT University issued computing accounts, it means that the individual agrees to obey with this and all other computing related policies. It is the accountability of the individual to keep oneself up-to-date on changes in the information

IT POLICY (Policy No. IIMTU/RO/IQAC/2022/27)

O. Pocket, Ganga Nagar, Mawana Road, Meerut. (U.P.) - 250001

Ph. No. 0121-2793500-506, Fax. 0121-2793600

Website : www.iimtu.com; E-mail : mail@iimtu.com



technology policy of IIMT University, Meerut and adjust to those changes as necessary from time to time.

10. Access to the IIMT University Network

Accessing Internet and Intranet of IIMT University.

- 1) A user shall register the client system and obtain one-time authorization from the competent authority before connecting the client system to the University Campus wide local area network.
- 2) IIMT University, Meerut shall sustain two independent networks, i.e. Internet and Intranet. Both the networks shall not have any physical connection/devices between them. End point compliance shall be implemented on both the networks to prevent not permitted access to data.
- 3) Users shall not carry out any activity through any website or applications to bypass filtering of the network or perform any other against the law acts which may harm the network's performance or security.

Accessing to IIMT University's Wireless Networks

For connecting to a IIMT University, Meerut's wireless network, user shall guarantee the following:

- 1) A user shall record the access device and obtain one-time authorization from the competent authority before connecting the access device to the IIMT University, Meerut's wireless network.
- 2) Wireless client systems and wireless devices shall not be permitted to connect to the IIMT University, Meerut wireless access points without due validation.
- 3) To ensure information security, it is suggested that users should not connect their devices to unsecured wireless networks.



IT POLICY (Policy No. IIMTU/RO/IQAC/2022/27)



Page 18

Filtering and blocking of sites:

- 1) Computer Centre or Implementing Agency may block content over the Internet which is in breach of the relevant provisions of the IT Act 2000 and other related laws or which may pose a security threat to the network.
- 2) Computer Centre or Implementing Agency may also block content which, in the opinion of the IIMT University, is wrong or may badly affect the productivity of the users.

11. Monitoring and Privacy

- 1) Computer Centre or Implementing Agency shall have the right to review networks and systems at regular intervals, from the point of agreement to this policy.
- 2) Implementing agency, for security related reasons or for conformity with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on the IIMT University provided devices under intimation to the user. This includes items such as files, electronic mails, posts on any electronic media, Internet history etc.
- 3) Implementing agency may check user's online activities on University network, subject to such Standard Operating Procedures of Government of India norms.

12. Electronic mail Access from the IIMT University Network

- 1) Electronic mail service authorized by IIMT University, Meerut and implemented by the Computer Centre shall only be used for all official correspondence.
- 2) More details in this regard are provided in the "Electronic mail usage policy of IIMT University, Meerut.

13. Access to Social Media Sites from IIMT University, Meerut Network.

Accessing Social networking sites by IIMT University, Meerut users are governed by Framework and Guidelines for use of Social Media for Government Organizations.

IT POLICY (Policy No. IIMTU/RO/IQAC/2022/27)

Page | 9

'O' Pocket, Ganga Nagar, Mawana Road, Meerut. (U.P.) - 250001

Ph. No. 0121-2793500-506, Fax. 0121-2793600

Website : www.iimtu.com; E-mail : mail@iimtu.com

- 2) User shall meet the terms with all the applicable provisions under the IT Act 2000, while posting any information on social networking sites.
- 3) User shall stick to the “Terms of Use” of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws.
- 4) User shall report any doubtful incident as soon as possible to the competent authority.
- 5) User shall at all times use high security settings on social networking sites.
- 6) User shall not place any material that is hateful, frightening, obscene, infringes copyright, insulting, hateful, pesky, harassment, discriminatory, racist, sexist, or is otherwise illegal.
- 7) User shall not reveal or use any confidential information obtained in their capacity as an employee of the IIMT University.
- 8) User shall not make any comment or post any material that might otherwise cause damage to IIMT University, Meerut’s reputation.

14. Use of Information Technology Devices Issued by IIMT University, Meerut

Information Technology devices issued by the IIMT University, Meerut to a user shall be primarily used for academic, research and any other University related purposes and in a lawful and ethical way and shall be governed by the practices defined in the Section “Use of information technology devices on IIMT University, Meerut network”. The abovementioned section covers best practices related to use of desktop devices, portable devices, external storage media and peripherals devices such as printers and scanners.

15. Security Incident Management Process

- 1) A security incident is defined as any undesirable event that can impact the availability, integrity, confidentiality and authority of IIMT University’s data.
- 2) Implementing agency reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system under intimation to the competent authority of the IIMT University.

IT POLICY (Policy No. IIMTU/RO/IQAC/2022/27)

Page | 10

- 3) Any security incident noticed must be immediately brought to the notice of the Indian Computer Emergency Response Team (ICERT) and the implementing agency.
- 4) Despite of anything in the above clause, the disclosure of logs relating to or contained in any information technology resource, to Law Enforcement agencies and other organizations by the implementing agency shall be done as per the IT Act 2000 and other applicable laws.
- 5) Implementing agency shall neither accept nor act on the request from any other organization, save as provided in this clause, for scrutiny or release of logs.

16. Intellectual Property of IIMT University, Meerut

Material accessible through the IIMT University, Meerut's network and resources may be subject to protection under privacy, promotion, or other individual rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use IIMT University, Meerut's network and assets in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

17. Enforcement

- 1) This policy document is applicable to all the users of IIMT University, Meerut as specified in Section 2 of this policy document. It is compulsory for all users to adhere to the provisions of this policy.
- 2) Each entity of IIMT University, Meerut shall be accountable for ensuring compliance with the provisions of this policy document. The Implementing Agency would make available necessary technical assistance to the user entities in this regard.

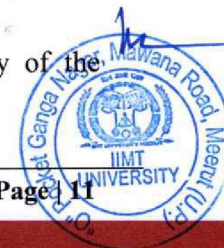
18. Deactivation

- 1) In case of any risk to security of IIMT University, Meerut's systems or network from the resources being used by a user, the resources being used may be deactivated immediately by the implementing agency.

Following to such deactivation, the concerned user and the competent authority of the University shall be informed.



IT POLICY (Policy No. IIMTU/RO/IQAC/2022/27)



Page 11

19. Audit of IIMT University, Meerut Network Infrastructure

The security audit of network infrastructure shall be conducted periodically by an organization approved by the University.

20. Review

Future changes in this Policy, as deemed necessary, shall be made by the Technical Committee of university with the approval of the Competent Authority of the University.

21. Information technology Hardware Installation Policy

University network user population needs to observe certain safety measures while getting their computers or peripherals installed so that he/she may face minimum problem due to interruption of services due to hardware failures.

A. Who is Primary User

An individual person in whose room the computer system is installed and is primarily used by him/her, is considered to be "primary" user. If a computer has multiple users, none of whom are considered as the "primary" user, the department HoD should make an arrangement and make a person accountable for conformity.

B. What are End User Computer Systems

Apart from the client personal computers used by the users, the IIMT University will consider servers not directly administered by Computer Centre, as end-user computers. If no primary user can be recognized, the department must presume the responsibilities identified for end-users. Computer systems, if any, that are acting as servers which provide services to other users on the IIMT University, Meerut Intranet/Internet though registered with the Computer Centre, are still considered under this policy as "end- users" computers.

C. Warranty & Annual Maintenance Contract

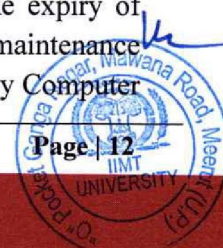
Computers purchased by any Section/ Department/ Project of IIMT University, Meerut should preferably be with one year onsite comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include standard repair and maintenance procedures as may be defined by Computer

IT POLICY (Policy No. IIMTU/RO/IQAC/2022/27)

G- Pocket, Ganga Nagar, Mawana Road, Meerut. (U.P.) - 250001

Ph. No. 0121-2793500-506, Fax. 0121-2793600

Website : www.iimtu.com; E-mail : mail@iimtu.com



Centre from time to time.

D. Power Connection to Computers and Peripherals

All the computers and peripherals should be connected to the electrical point strictly through uninterrupted power supply. Power supply to the uninterrupted power supply should never be switched off, as continuous power supply to uninterrupted power supply is required for battery recharging, till such instances wherein the uninterrupted power supply is to be left unattended. Further, these uninterrupted power supply systems should be connected to the electrical points that are provided with proper earthing and have properly laid electrical wiring.

E. Network Connection

While linking the computer to the network, the connecting networking cable should be at a distance from any electrical/electronic equipment, as they interfere with the network communication. Additionally, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

F. File and Print Sharing Facilities offered by IIMT University

File and print sharing services on the computer over the network should be installed only when it is extremely required. When files are shared through network, they should be protected with password and also with read only access rule.

G. Maintenance of Computer Systems provided by the IIMT University

For all the computers that were purchased by the IIMT University centrally and distributed by Computer Centre will attend to the complaints related to any maintenance related problems.



22. Software Installation and Licensing Policy of IIMT University, Meerut

Any computer purchases made by the individual Schools / departments/projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed in the computer systems.

Respecting the anti-piracy laws of the India, IIMT University information technology policy doesnot allow any pirated/not permitted software installation on the IIMT University owned computers and the computers connected to the IIMT University campus network. In case of any such instances, IIMT University will hold the School/department/individual personally responsible for any pirated software installed on the computers located in their School/department/individuals' rooms.

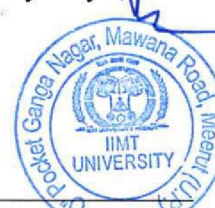
A. Operating System and its Updating policy in IIMT University, Meerut

Individual users should make sure that respective computer systems have their operating system updated in respect of their service packs/patches, through internet. Checking for updates and updating of the operating system should be performed at least once in a week or as suggested by computer center.

IIMT University as a policy encourages user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.

B. Use of software on Desktop systems in IIMT University, Meerut

- a. Users shall not copy or install any software on their own on their desktop systems, including privately owned shareware and freeware without the approval of the competent authority of IIMT University, Meerut.
- b. Any software installed should be used for activities of the IIMT University only.



C. Antivirus Software and its updating

Computer systems used in the IIMT University should have anti-virus software installed, and it should be dynamic at all the times. The primary user of a computer system is accountable for keeping the computer system compliant with this virus protection policy.

Individual users should make sure that respective computer systems have current virus protection software installed and maintained.

D. Backups Data for IIMT University

Individual users should perform regular backups of their crucial data. Users should keep their valuable data backups in external storage devices such as pen drives, external hard disks etc.

23. Use of Information technology devices on IIMT University, Meerut network

This section provides the best practices related to use of desktop devices, portable devices, external storage media and peripheral devices such as printers and scanners on IIMT University's network.

Desktop Devices present in IIMT University, Meerut

1) Use and Ownership

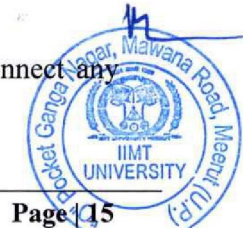
Desktops shall as a rule be used only for transacting IIMT University's works. Users shall use their own good judgment and discretion towards use of desktop devices for personal use to the minimum extent possible.

2) Security and Proprietary Information

Users shall take prior approval from the implementing agency to connect any access device to the IIMT University's network.



IT POLICY (Policy No. IIMTU/RO/IQAC/2022/27)



Page 15

- b. User shall keep their passwords protected and not share their account details to anybody. Users shall keep strong and secure passwords as per the password policy of the application.
- c. All active desktop computers shall be secured with a password-protected screensaver which should be set with automatic activation at 5 minutes or less, or log-off when the system is unattended.
- d. Users shall ensure that updated virus-scanning software is running all time, in all systems. Users shall exercise due caution when opening e-mail attachments received from unknown senders as they may contain viruses, e-mail bombs, or Trojan horse code.
- e. User shall report any loss of data or accessories to the implementing agency and competent authority of IIMT University, Meerut.
- f. User shall obtain approval from the competent authority before taking any IIMT University, Meerut issued desktop outside the premises of the IIMT University.
- g. Users shall accurately shut down the systems before leaving the School/department/office.
- h. Users shall abide by instructions or procedures as directed by the Computer Centre from time to time.
- i. If users infer that their computer has been infected with a virus (e.g. it might have become erratic or time-consuming in response), it should be reported to the implementing agency (Computer Centre) for remedial action.

Sharing of data in IIMT University, Meerut

Users shall not distribute their credentials to anyone in IIMT University, Meerut.

Use of Portable devices in IIMT University, Meerut

Devices covered under this segment include IIMT University , Meerut issued laptops, mobiles, iPads, tablets, Personal digital assistants etc. Use of the devices shall be governed by the following:



IT POLICY (Policy No. IIMTU/RO/IQAC/2022/27)



Page | 16

- a. User shall be held responsible for any unlawful usage of their IIMT University, Meerut issued access device by a third party.
- b. Users shall keep the IIMT University, Meerut issued devices with them at all times or store them in a protected location when not in use. User should not leave the devices unattended in public locations.
- c. User shall ensure that the portable devices are password protected and auto lockout enabled. The password used should be as strong as the device may support and should be as per the password policy of the application.
- d. Computer Centre shall ensure that the latest operating system, anti-virus and application patches are available on all the devices, in coordination with the User. Firewalls shall be enabled, if possible.
- e. Users shall wipe or securely delete data from the device before returning/dropping it off.
- f. Lost, stolen, or misplaced devices shall be immediately reported to the IA/ and the competent authority.
- g. When installing software, user shall review the application permissions to ensure that unwanted information regarding the user is not shared with the application provider.

24. Network (Intranet & Internet) Use Policy

Network connectivity provided through the IIMT University, referred to hereafter as "the Network", either through an authentic network access connection or a Virtual Private Network (VPN) connection, is governed under the IIMT University IT Policy. The Computer Centre is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the IIMT University's network should be reported to Implementing agency / Computer Centre.

A. IP Address Allocation in IIMT University

Any workstation (PC/Server) that will be connected to the IIMT University network, should have an IP address assigned by the Computer Centre. Subsequently a systematic approach, the range of IP addresses that will be allocated will be based on Virtual LAN

IT POLICY (Policy No. IIMTU/RO/IQAC/2022/27)

'O' Poch, Ganga Nagar, Mawana Road, Meerut. (U.P.) - 250001

Ph. No. 0121-2793600-506, Fax. 0121-2793600

Website: www.iimtu.com; E-mail: mail@iimtu.com

created against each entity. Any device connected to the network will be allocated IP address only from that address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorized from any other location.

As and when a new PC is installed in any location, it will be owed as per the DHCP pool policies.

An IP address allocated for a particular PC system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. IP address for each computer should be obtained separately by filling up a requisition form meant for this intention.

B. DHCP and Proxy Configuration by Individual Schools/Departments.

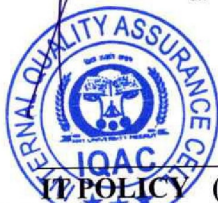
Use of any workstation at end user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should be strictly avoided, as it is considered to be absolute violation of IP address allocation policy of the University. Similarly, arrangement of proxy servers should also be avoided, as it may interfere with the services run by the Computer Centre.

Even arrangement of any computer with additional network interface card and connecting another computer to it is considered as proxy/DHCP configuration.

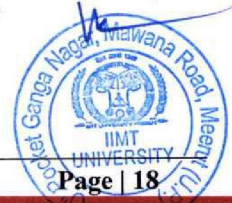
Nonconformity to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the network. Connection will be restored after receiving written assurance of compliance from the concerned School/department.

C. Running Network Services on the Servers

- a. Individual Schools/departments/individuals connecting to the IIMT University network over the LAN may run server software.



IT POLICY (Policy No. IIMTU/RO/IQAC/2022/27)

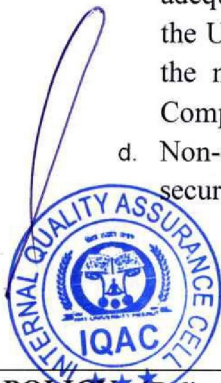


Page | 18

- b. Computer Centre takes no responsibility for the content of machines connected to the Network, regardless of those machines being University or personal property.
- c. Computer Centre will be constrained to disconnect client machines where potentially damaging software is found to exist.
- d. Access to remote networks using a University's network connection must be in compliance with all policies and rules of those networks.
- e. Network traffic will be monitored for security and for performance reasons at Computer Centre.
- f. Imitation of an authorized user while connecting to the Network is in direct violation of this policy and will result in the termination of the connection.

D. Internet Bandwidth obtained by Other Schools/Departments of IIMT University.

- a. Internet bandwidth acquired by any School/Department of the University under any research programme/project should ideally be pooled with the University's Internet bandwidth, and be treated as University's common resource.
- b. Under particular circumstances, which prevent any such pooling with the University Internet bandwidth, such network should be totally separated from the University's campus network. All the computer systems using that network should have separate VLANs based on grouping criterion.
- c. IP address scheme (private as well as public) and the University gateway should not be specified as alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the University IT policy. One copy of the network diagram giving the details of the network design and the IP address schemes used may be submitted to Computer Centre.
- d. Non-compliance to this policy will be direct violation of the University's IT security policy.



25. Email Account Usage Policy

IIMT University provides official email access privileges to its users. In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the IIMT University's administrators, it is suggested to utilize the University's e-mail services, for formal University communication and for academic & other official purposes.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

- 1) The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
 - 2) Using the facility for illegal/commercial purposes is a direct violation of the University's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
 - 3) While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
 - 4) User should keep the mail box used space within about 75 % usage threshold, as 'mailbox full' or 'mailbox almost full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
 - 5) User should not open any mail or attachment that is from unidentified and doubtful source. Even if it is from known source, and if it contains any attachment that is of doubtful in nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have potential to damage the valuable information on your computer.
 - 6) User should not share his/her email account's credentials with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
- User should abstain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.



- 8) While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.
- 9) Impersonating email account of others will be taken as a serious offence under the IT security policy.
- 10) It is finally each individual's responsibility to keep their e-mail account free from violations of IIMT University's email usage policy.
- 11) All the Emails detected as spam mails go into SPAM folder of the respective users' mailaccounts. Users are requested to open these folders periodically to check any important mail wrongly stamped as SPAM mail and went into this folder. It is suggested to empty this folder as frequently as possible.

The above laid down policies particularly 1 to 11 are largely applicable even to the email services that are provided by other service providers such as RediffMail, Gmail, Hotmail, Yahoo, etc., as long as they are being used from the IIMT University's campus network, or by using the resources provided by the University to the individual for official use even from outside.

26. Institutional Repository (IR)

IIMT University, Meerut shall be providing services related to Institutional Repository (IR) through Central Library of the University as per the following policies:

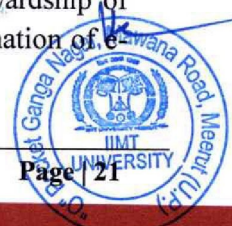
What is IR (Institutional Repository)?

A University institutional repository (IR) is a set of services that a University Library offers to the members of its group of people for the management and dissemination of digital materials created by the IIMT University or institution and its community members. It is most essentially an organizational commitment to the stewardship of these digital materials including long-term preservation, access and dissemination of e-resources of an organization to its users.

IT POLICY (Policy No. IIMTU/RO/IQAC/2022/27)

'O' Pocket, Ganga Nagar, Mawana Road, Meerut. (U.P.) - 250001
Ph. No. 0121-2793500-506, Fax. 0121-2793600

Website : www.iimtu.com; E-mail : mail@iimtu.com



What Does IR contain?

IR of the institution contains a wide variety of documents depending on the policy of the institution.

Who will be entitled to access IIMT University, Meerut IR?

Faculty members/ Research scholars/Students and other staff members having institutional e- mail IDs are authorized members to access the IR of IIMT University, Meerut.

How will you access the IR?

The registered members through their institutional e-mail address can access the IPR.

Validity Period of Accessibility of IR

Teachers/Researchers/ Students are allowed to access IIMT University, Meerut IR as long as they are stakeholders in the University.

Copyright Violation on IR Use

IIMT University, Meerut IR digital materials are mainly grey literature. Any downloaded materials from the IR come under the purview of copyright. The downloaded materials cannot be reprinted and used for commercial purpose further. If any member found violating such copyright act shall be treated as per the provisions of copyright act-1957.



27. Disposal of ICT equipment

The discarding of ICT hardware equipment shall be done as per the Standard Operating Procedures of the E-Waste Management of the IIMT University.

At IIMT University, Meerut, use of ICT facilities have been encouraged. In view of these scenarios, IIMT University, Meerut intends to provide budgetary provisions as follows:

- 1) Budgetary provisions should be made under recurring grants to maintain the entire existing ICT infrastructure.
- 2) Sufficient budgetary provisions under capital head should be kept for up gradation and addition to ICT infrastructure.
- 3) Budgetary provisions under capital grants should also be allocated for implementation of newer ICT solutions from time to time.
- 4) In IIMT University, Meerut there has been an increase of 10% enrolment of students every year. Keeping in view of this increase, a budget of 10% of the total budget of the University should be earmarked for ICT facility particularly for students.

28. Breach of this Policy

Users are encouraged to be watchful and to report any alleged violations of this policy immediately to the implementing agency.

If any breach of this Policy is observed, then the disciplinary action may be taken in accordance with the University's disciplinary procedures.

29. Revisions to Policy

The IIMT University, Meerut reserves the right to revise the terms of this Policy at any time. Any such revisions will be available on the IIMT University, Meerut website and by continuing to use the IIMT University's information technology resources following any update it is considered acceptance on the revised terms of this policy.

Appendix – I: Email Requisition Form

FORM FOR REQUISITION OF OFFICIAL EMAIL ID

(For Teachers & Staff only)

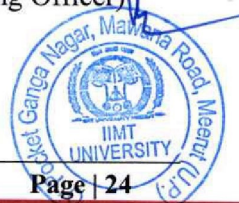
First Name	:
Middle Name	:
Last Name	:
Department/ Branch	:
Current Emailaddress*	:
Mobile Number	:

Note:

1. Please spell the names and all other information sought above correctly.
2. *This Email address should be currently used by you.
3. The filled in form should be submitted after getting duly signed from respective Head of the Department/ Controlling Officer.
4. An official Email address would be created within 48 hrs. - 72 hrs.
5. Information regarding the official Email address created would be sent to your current Email address.

GRANT AN OFFICIAL E-MAIL ID PLEASE.

(Signature of the Head of the Department/ Controlling Officer)



IT POLICY (Policy No. IIMTU/RO/IQAC/2022/27)

'O' Pocket, Ganga Nagar, Mawana Road, Meerut. (U.P.) - 250001
Ph. No. 0121-2793500-506, Fax. 0121-2793600

Website : www.iimtu.com; E-mail : mail@iimtu.com

Appendix – II: Email Requisition Form

FORM FOR REQUISITION OF OFFICIAL EMAIL ID

(For Research Scholars only)

First Name	:
Middle Name	:
Last Name	:
Department	:
Name of the PI	:
Name of the Project	:
Duration of Research	:
Current Emailaddress*	:
Phone Number	:
Admission Year*	:

Note:

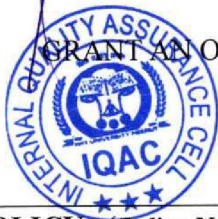
1. Please spell the names and all other information sought above correctly.
2. *This Email address should be currently used by you.
3. The filled in form should be submitted after getting duly signed from respective Head of the Department and Principal Investigator.
4. An official Email address would be created within 48 hrs. - 72 hrs.
5. Information regarding the official Email address created would be sent to your current Email address.

GRANT AN OFFICIAL E-MAIL ID PLEASE.

(Signature of the Head of the Department)

GRANT AN OFFICIAL E-MAIL ID PLEASE.

(Signature of the Head of the Department)



IT POLICY (Policy No. IIMTU/RO/IQAC/2022/27)

'O' Pocket, Ganga Nagar, Mawana Road, Meerut. (U.P.) - 250001

Ph. No. 0121-2793500-506, Fax. 0121-2793600

Website : www.iimtu.com; E-mail : mail@iimtu.com



Appendix – III: Wi-Fi Access Requisition Form

FORM FOR REQUISITION OF WI-FI ACCESS

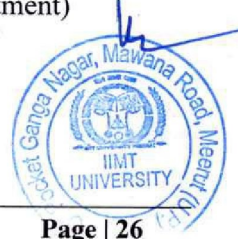
(For Students only)

Name	:	
Father's Name	:	
Gender	:	
DoB	:	
Department	:	
Course	:	
Semester	:	
Roll No.	:	
Email address*	:	
Mobile Number	:	

Note:

1. Please spell the names and all other information sought above correctly.
2. *This Email address should be currently used by you.
3. The filled in form should be submitted after getting duly signed from respective Head of the Department.

(Signature of the Head of the Department)



IT POLICY (Policy No. IIMTU/RO/IQAC/2022/27)

Page | 26

'O' Pocket, Ganga Nagar, Mawana Road, Meerut. (U.P.) - 250001

Ph. No. 0121-2793500-506, Fax. 0121-2793600

Website : www.iimtu.com; E-mail : mail@iimtu.com

Appendix – IV: IIMT University, Meerut Wi-Fi
Access Requisition Form

FORM FOR REQUISITION OF WI-FI ACCESS

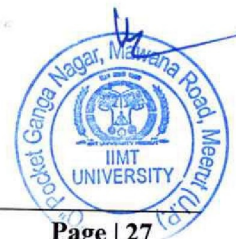
(For Employees only)

Name	:	
Father's Name	:	
Gender	:	
DoB	:	
Department/ Branch	:	
Email address*	:	
Mobile Number	:	

Note:

1. Please spell the names and all other information required above correctly.
2. *This Email address should be currently used by you.
3. The filled in form should be submitted after getting duly signed from respective implementing agency.

(Signature of the Controlling Officer)



IT POLICY (Policy No. IIMTU/RO/IQAC/2022/27)

'O' Pocket, Ganga Nagar, Mawana Road, Meerut. (U.P.) - 250001
Ph. No. 0121-2793500-506, Fax. 0121-2793600

Website : www.iimtu.com; **E-mail :** mail@iimtu.com